UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/092,973	03/07/2002	Jean-Claude Junqua	9432-000148	1465

27572 7590 09/22/2006

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 828
BLOOMFIELD HILLS, MI 48303

EXAMINER	
YEN, ERIC L	

ART UNIT	PAPER NUMBER
2626	

DATE MAILED: 09/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/092,973	**Applicant(s)** JUNQUA, JEAN-CLAUDE
	Examiner Eric Yen	**Art Unit** 2626

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 June 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. In response to the Office Action mailed 2/28/06, applicant has submitted an amendment filed 7/28/06.

Claims 1, 21, and 28, have been amended. New Claim 31 has been added.

Request for Telephonic Interview Cancelled

The examiner contacted Applicant's representative Jennifer S. Brooks regarding the request for a telephonic interview on approximately 7/21/06. The interview that was scheduled to occur the following day was cancelled by applicant's representative, in order to contemplate applicant's instructions to abandon the case. No further indication that an interview would be requested in the future was provided.

Response to Arguments

2. Applicant's arguments with respect to claims 1, 21, and 28, have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-15, 17-20, and 28-29, are rejected under 35 U.S.C. 103(a) as being unpatentable over Traynor (US 2002/0007278), in view of Carter et al. ("An Integrated Biometric Database"), hereafter Carter.

As per Claim 1, Traynor teaches an apparatus for interacting with a secure resource accessible through a telephone system of the type that provides telephone access through a plurality of extensions, comprising:

a security server having an interface for sending messages to said telephone system, said messages being adapted to provide control signals to said secure resource ("web server...secure transactions...voice print...speech activated", paragraph 19; "telephone call...authenticating", paragraph 10; Figure 1, elements 110 and 120)

a biometric data store that stores biometric data associated with at least one user ("information specific for each remote appliance and for each caller", paragraph 19)

a biometric data input system coupled to said security server and operable to obtain an utterance from said user ("telephone...transmits their voice through the callers network...server...verification", paragraph 18)

and a biometric verification/identification system being configured to generate a first confidence level based on a text independent component of said utterance, to access said data store, to evaluate said text independent component of said utterance vis-à-vis said stored biometric data, and to provide instructions to said security server and thereby provide control signals for interacting with said secure resource ("verifies the caller's voice", paragraph 15; "voice profile… coupled with the caller's own PIN number", paragraph 18; "controlling…calling into the…server…turn off the ignition", paragraph 16)

and at least two of the extensions being associated with biometric data ("contains information specific for each remote appliance and for each caller…voice print", paragraph 19)

Traynor fails to teach wherein said verification/identification system is adapted to access a data structure storing associations among different types of biometric data and individual ones of said extensions, in order to retrieve stored biometric data associated with an extension being operated by a user, and where the biometric data that the at least two of the extensions are associated with are different types of biometric data.

Carter teaches wherein said verification/identification system is adapted to access a data structure storing associations among different types of biometric data and individual ones of said extensions, in order to retrieve stored biometric data associated with an extension being operated by a user, and where the biometric data that the at least two of the extensions are associated with are different types of biometric data ("speech, signature and face…human confirmation of the speaker…voice recording…signature…face images", page 2, paragraph 3; Carter teaches different types of biometric data and Traynor teaches that each extension has its own data, and so each extension is associated with its own different types of biometric data [such as face, voice, etc.])

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify Traynor to include the teaching of Carter of wherein said verification/identification system is adapted to access a data structure storing associations among different types of biometric data and individual ones of said extensions, in order to retrieve stored biometric data associated with an extension being operated by a user, and where the biometric data that the at least two of the extensions are associated with are different types of biometric data, in order to provide personal identification data to verify identify, as described by Carter (page 1, paragraph 1).

As per Claim 28, the limitations are similar to those in Claim 1, and so is rejected under similar rationale.

As per Claim 2, Traynor teaches wherein said interface is a telephony interface coupled to said telephone system (Figure 1).

As per Claim 3, Traynor teaches wherein said interface is an interface coupling said security server with an intermediate system that in turn communicates with said telephone system (Figure 1).

As per Claim 4, Traynor teaches wherein said interface is a network interface for communicating messages over a network between said security server and said telephone system (Figure 1).

As per Claim 5, Traynor teaches wherein said data store is configured to store biometric data in association with at least one of said plurality of extensions ("voice profile...each remote applicance and for each caller", paragraphs 18-19)

As per Claim 6, Traynor teaches wherein said biometric data input system is operable to obtain user biometric data from a user operating one of said plurality of extensions ("enroll", paragraph 18).

As per Claim 7, Traynor teaches wherein said security system is configurable through training to operate upon biometric data from said user ("authenticating", paragraph 10; "enroll", paragraph 18; "voice print", paragraph 19).

As per Claim 8, Traynor teaches wherein said security system is configurable through training to operate upon biometric data from said user using training speech provided using said telephone system ("enroll", paragraph 18).

As per Claim 9, Traynor teaches wherein said security system includes direct interface for coupling to said secure resource (Figure 1).

As per Claim 10, Traynor teaches wherein said direct interface is a wired connection to said secure resource (Figure 1).

As per Claim 11, Traynor teaches wherein said direct interface is a network connection communicating with said secure resource (Figure 1).

As per Claim 12, Traynor teaches wherein said direct interface is a wireless connection communicating with said secure resource (Figure 1).

As per Claim 13, Traynor teaches wherein said biometric data input system is a voice input system (“voice commands”, paragraph 9).

As per Claim 14, Traynor teaches wherein said biometric data input system is a voice input system communicating with said telephone system through at least one of the extensions (“voice commands”, paragraph 9; “verification”, paragraph 18; Figure 1).

As per Claim 15, Traynor teaches wherein said biometric verification/identification system employs a speaker verification/identification system (“voice verification”, paragraph 18).

As per Claim 17, Traynor teaches wherein said biometric verification/identification system employs a speech recognition system that compares a text dependent component of said utterance with a predefined list of keywords (“Pepsi, Sprite, Gingerale”, paragraph 15).

As per Claim 18, Traynor teaches wherein said biometric verification/identification system employs a speech recognition system that employs a wordspotting system for identifying keywords within said utterance ("Pepsi, Sprite, Gigerale", paragraph 15).

As per Claim 19, Traynor teaches wherein said biometric verification/identification system employs a speaker verification/identification system that assesses at least one text dependent component of said utterance ("voice profile...PIN", paragraph 18, "label ID...spoken...query...Pepsi", paragraph 15).

As per Claim 20, Traynor teaches wherein said security server couples to said telephone system as one of said plurality of extensions (Figure 1).

As per Claim 29, Traynor teaches storing biometric data associated with a plurality of users ("each caller...callers voice print", paragraph 19).

5. Claims 21-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Traynor, in view of Hoskinson et al. (US 5,339,351), Li et al. (US 6,219,793), hereafter Li, and Carter.

As per Claim 21, Traynor teaches a method of interacting with a secure resource accessible through a telephone system of the type that provides telephone acess through a plurality of extensions comprising the steps of:

receiving user biometric data from a user operating one of said extensions ("enroll", paragraph 18; Figure 1; "voice print", paragraph 19)

evaluating said user biometric data vis-à-vis said stored biometric data (application verifies caller's voice, paragraph 15; voice profile used for voice verification, and voice profile is coupled with caller's PIN, paragraph 18)

providing instructions to interact with said secure resource based on the results of said evaluating step (uses, paragraph 16; "bill the caller", paragraph 19; "voice verification in future transactions", paragraph 18)

and at least two of the extensions being associated with biometric data ("contains information specific for each remote appliance and for each caller...voice print", paragraph 19).

Traynor fails to teach associating said plurality of extensions with a plurality of fixed locations, and obtaining user extension information that identifies which one of said fixed physical locations the user is located.

Hoskinson teaches associating said plurality of extensions with a plurality of fixed locations, and obtaining user extension information that identifies which one of said fixed physical locations the user is located (location identification, Abstract).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify Traynor to include the teaching of Hoskinson of associating said plurality of extensions with a plurality of fixed locations, and obtaining user extension information that identifies which one of said fixed physical locations the user is located, in order to provide location information to a system that requires it, as described by Hoskinson (col. 2, lines 28-32).

Traynor, in view of Hoskinson, fail to teach using said user extension information and sad biometric data to access a data store containing stored biometric data associated with stored extension information.

Li teaches using said user extension information and said biometric data to access a data store containing stored biometric data associated with stored extension information (caller ID and terminal ID are jointly authenticated, col. 16, lines 16-34; col. 17, lines 22-35).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify Traynor to include the teaching of Li of using said user extension information and sad biometric data to access a data store containing stored biometric data associated with stored extension information, in order to achieve a higher level of security in phone networks, as described by Li (col. 16, lines 32-34).

Traynor, Hoskinson, and Li, fail to teach including accessing a data structure storing associations among different types of biometric data and individual ones of said extensions, in order to retrieve stored biometric data associated with an extension being operated by a user, and where the biometric data that the at least two of the extensions are associated with are different types of biometric data.

Carter teaches including accessing a data structure storing associations among different types of biometric data and individual ones of said extensions, in order to retrieve stored biometric data associated with an extension being operated by a user, and where the biometric data that the at least two of the extensions are associated with are different types of biometric data ("speech, signature and face...human confirmation of the speaker...voice recording...signature...face images", page 2, paragraph 3; Carter teaches different types of biometric data and Traynor teaches that each extension has its own data, and so each extension is associated with its own different types of biometric data [such as face, voice, etc.])

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify Traynor to include the teaching of Carter of including accessing a data structure storing associations among different types of biometric data and individual ones of said extensions, in order to retrieve stored biometric data associated with an extension being operated by a user, and where the biometric data that the at least two of the extensions are associated with are different types of biometric data, in order to provide personal identification data to verify identify, as described by Carter (page 1, paragraph 1).

As per Claim 22, Traynor teaches wherein said biometric data is speech data ("voice", paragraph 18).

As per Claim 23, Traynor teaches wherein said biometric data is speech data provided through said one of said extensions "enroll", paragraph 18).

As per Claim 24, Traynor teaches wherein said biometric data is speech data and said evaluating step includes determining whether said speech data is associated with said one of said extensions the user is operating (recognizing and authenticating, paragraphs 10 and 18).

As per Claim 25, Traynor teaches wherein said biometric data is speech data and said evaluating step is performed using a speaker recognition to compare said speech data with a predefined set of keywords (voice profile is coupled with caller's own PIN number, paragraph 18; pepsi, sprite, gingerale, paragraph 15).

As per Claim 26, the limitations are similar to those in Claim 18, and so is rejected under similar rationale.

As per Claim 27, Traynor teaches wherein said biometric data is stream of continuous speech data and said evaluating step is performed by assessing at least one text independent component and at least one text dependent component (voice profile coupled with caller's own PIN number, paragraph 18; user speaks appliance's label and voice is verified and query recognized, Pepsi, Sprite, Gingerale, paragraph 15)

6. Claims 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Traynor, in view of Carter, as applied to Claim 1, above, and further in view of Li.

As per Claim 16, Traynor fails to teach wherein said biometric verification/identification system automatically determines an extension identifier associated with said one of said plurality of extensions being operated by said user, and uses said extension identifier in accessing said stored biometric data.

Li teaches wherein said biometric verification/identification system automatically determines an extension identifier associated with said one of said plurality of extensions being operated by said user, and uses said extension identifier in accessing said stored biometric data (caller ID and terminal ID are jointly authenticated, col. 16, lines 16-34; col. 17, lines 22-35).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify Traynor to include the teaching of Li of wherein said biometric verification/identification system automatically determines an extension identifier associated with said one of said plurality of extensions being operated by said user, and uses said extension identifier in accessing said stored biometric data, in order to achieve a higher level of security in phone networks, as described by Li (col. 16, lines 32-34).

7. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Traynor, in view of Carter, as applied to Claim 1, above, and further in view of Namba et al. (US 5,884,249), hereafter Namba.

As per Claim 30, Traynor, in view of Carter, fail to teach wherein said apparatus is adapted to switch, in response to receipt of an utterance from said user from at least one of said extensions, from a manual entry mode to an automatic entry mode permitting hands-free gaining of access by the user to the secure resource by providing only voice-based data entry, wherein said manual entry mode permits the user to gain access to the secure resource without automated, voice-based user authentication.

Namba teaches wherein said apparatus is adapted to switch, in response to receipt of an utterance from said user from at least one of said extensions, from a manual entry mode to an automatic entry mode permitting hands-free gaining of access by the user to the secure resource by providing only voice-based data entry, wherein said manual entry mode permits the user to gain access to the secure resource without automated, voice-based user authentication (system is programmed to automatically switch between plural inputting means, including voice or manual operation, hence in order to switch from a manual operation mode to a voice mode the user changes the input mode to a voice one by inputting voice data, col. 5, lines 21-26).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify Traynor, in view of Carter, to include the teaching of Namba of wherein said apparatus is adapted to switch, in response to receipt of an utterance from said user from at least one of said extensions, from a manual entry mode to an automatic entry mode permitting hands-free gaining of access by the user to the secure resource by providing only voice-based data entry, wherein said manual entry mode permits the user to gain access to the secure resource without automated, voice-based user authentication, in order to provide an input managing method when simultaneously using plural input means in information processing equipment, as described by Namba (col. 1, lines 9-13).

8. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Traynor, in view of Carter, as applied to Claim 1, and further in view of Lewis (US 6,213,391).

As per Claim 31, Traynor, in view of Carter, fail to teach wherein associations between the different types of biometric data and the individual extensions are configured to ensure that said verification/identification system selectively retrieves only those types of stored biometric data that are capable of being measured by security access control equipment at a physical location of the extension and in communication with the extension.

Lewis suggests wherein associations between the different types of biometric data and the individual extensions are configured to ensure that said verification/identification system selectively retrieves only those types of stored biometric data that are capable of being measured by security access control equipment at a physical location of the extension and in communication with the extension ("voice pattern identification profile...compared to the user's actual voice profile for match", col. 7, lines 34-59; "secondary means of identification...fingerprint profile", col. 9, lines 6-19; "cellular phones...PDAs", col. 6, lines 14-31; "verifying means...voice sample, fingerprint sample, digital signature...fetches the authorized identification profile(s)...compares it to the spontaneously created profile", col. 10, lines 1-23; Lewis teaches secondary verification and retrieval of actual user profiles ['profile(s)' in col. 10, lines 1-23, includes multiple profiles] dedicated to a particular input measured by the device. Therefore, in one embodiment, the profiles retrieved are for more than one type of input [e.g., the fingerprint profile and the voice profile, as primary and secondary verification], or one type of input [e.g., the example where only voice verification is performed, in which case only the voice profile is retrieved for verification purposes]).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to modify Traynor, in view of Carter, to include the teaching of Lewis of wherein associations between the different types of biometric data and the individual extensions are configured to ensure that said verification/identification system selectively retrieves only those types of stored biometric data that are capable of being measured by security access control equipment at a physical location of the extension and in communication with the extension, in order to provide improved security, portability, and ease of flexibility of use, as described by Lewis (col. 3, lines 36-46).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Murviet et al. (US 7,058,573), Bakis et al. (US 6,219,639), Mihara et al. (US 6,504,944).

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eric Yen whose telephone number is 571-272-4249. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Talivaldis Smits can be reached on 571-272-7628. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EY 9/11/06

TĀLIVALDIS IVARS ŠMITS
PRIMARY EXAMINER